1-2 December 2005 • Kowloon Shangri-La Hotel • Hong Kong

2005 亞太風險管理與安全研討會

Asia-Pacific Conference on Risk Management and Safety

Challenges in Engineering Applications and Advances in Technologies

Proceedings

Organised by

HKARMS 香港風險管理與安全協會 Hong Kong Association of Risk Management and Safety

with

City University of Hong Kong

Occupational Safety & Health Council

職業安全健康局 Occupational Safety & Health Council

2005 Asia-Pacific Conference on Risk Management and Safety

PROCEEDINGS

Organised by

Hong Kong Association of Risk Management and Safety

In association with

City University of Hong Kong

Occupational Safety and Health Council

Evaluation of Human Factor within System Reliability

Martino Bandelloni , Filippo De Carlo , Orlando Borgia , and Francesca Tocchi *[1]
University of Florence, Energetic Department "Sergio Stecco" , Florence, Italy

Abstract: The increasing number of accidents and the growing complexity of system technologies lead to the consequence that theoretical models not considering human factor aren't able to fully explain real events. Understanding and evaluating the influence of human factor is necessary to assess its weight on the overall system performance.

The present work is based on the cognitive model used by CREAM technique - Cognitive Reliability and Error Analysis Method. CREAM offers a cognitive model and its application methodology in a practical approach to performance analysis and prediction of human reliability.

The main goal of this study is the proposal of a modeling technique based on a user-friendly graphic representation introducing human reliability main elements and their interactions. In a second time, such a model has been easily implemented by means of a special purpose simulation software called SPAR (™ of Clockwork Group), conceived and used in reliability, availability and logistic support assessment. A first application was performed developing simulation runs, based on simple assumptions about human performance and analyzing the results.

Keywords: Human Reliability, system reliability, simulation

1. THE ROLE OF HUMAN FACTOR IN SYSTEM RELIABILITY ASSESSMENT

During the last years many incidental events have happened in industrial systems. They often imply many damages for plants, environment and people as well an important performance and safety reduction. An efficient reliability assessment has the aim of avoiding or at least reducing, the possible damages consequent to a failure, analysing the overall system plant. In fact the overall reliability of a complex system can be assessed by means of a complete analysis of all the aspects characterizing and influencing its the global state. Hence it's clear that human factor analysis assumes a fundamental role: it can increase safety because it helps to evaluate and reduce human errors.

At the very beginning of these studies, human error assessment was performed using methods derived from PSA – Probabilistic Safety Assessment. These techniques identify and calculate accidents probabilities and frequencies putting the attention only on mechanical components. Human beings are modelled as mechanical components or not considered at all.

Only HRA– Human Reliability Analysis [1] [2], during the fifties, put the attention on the human factor considering performance variability, man-machine interaction and operator control over the system. Up to now many methodologies have been developed to help evaluating human reliability following the way undertaken by the HRA. At the beginning HRA took into consideration PSA principles, giving rise to the *1st generation methodologies*. These assign to human errors a probabilistic distribution to use in quantitative techniques such as Fault Tree Analysis and so on. Quantitative methodologies represent man as a mechanical component since they are not able to consider dynamic interactions with environment, social context and physical aspects. Moreover in such models there isn't a global approach, considering mutual interactions among man, technology and organization *(MTO – Man, Technology & Organization)* and therefore they aren't able to provide a wide-ranging representation of a dynamic real systems.

[1] Email of Francesca Tocchi : Francesca.tocchi@siti.de.unifi.it

The evolution of the first kind of models are the *2nd generation methodologies* that, briefly, consist of a qualitative assessment and a way of modeling the system which is more coherent with the real state of the system and more bound to the operator behaviour. These models are the cognitive ones, capable of considering the interactions of man, social, physical and environmental elements with the mechanical system, with a greater qualitative nature. Since they consider the human element not as a mechanical and static component but as a dynamic entity, it's necessary a cognitive model to substitute quantitative techniques used by *1st generation methodologies*. A cognitive model is defined as a modeling techniques able to analyze and represent human knowledge within a working system. In other words a cognitive model is parametric representation of human behaviour. A consistent model of human cognition is one of the most important and critical to be represented. A cognitive model is used to define the way in which actions are typically produced by human minds and can help in realizing the way how erroneous actions may come out. In the last years many cognitive models have been proposed to the scientific community, trying to represent in a better way all the possible dynamics of human behavior. The cognitive model used for the present study derives from SMoC (Simple Model of Cognition). It uses four basic cognitive functions which are Observation, Interpretation, Planning and Execution in order to represent the process followed to fulfill any task. In SMoC cognition has a cyclic nature: hierarchical classifications does not exist, cognition is a process in continuous evolving. Moreover, starting from a cognitive model, it is possible to assess which is the cognitive demand for a specific procedure and which is the corresponding cognitive available profile of the operator.

2. THE MODEL

The main goal of this study is the proposal of a modelling technique able to represent human factor elements inside the reliability assessment of a control system. For a mixed man-machine system, quantifying reliability performances is very difficult because, at the present moment, there isn't any model representing numerically human influence.

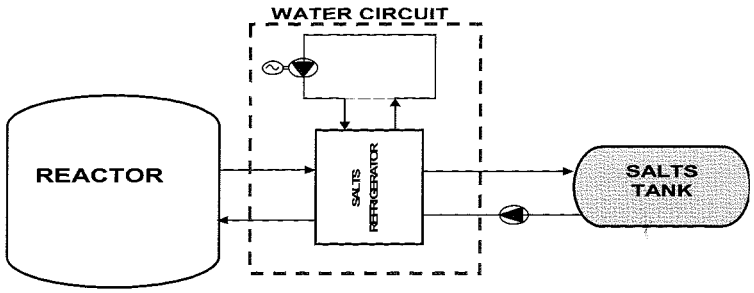
Let us consider a system composed by some process components and a control device monitoring that process. The reliability of the electromechanical system is appraisable using the well known techniques, such as RBDs, etc.. Regarding the other part of the system, the introduction of operators with control tasks, would involve consequences in terms of reliability variation which we'd like to evaluate. The links between operators and the plant's physical components are the operative procedures. Their analysis and study was chosen as the way to model and structure the man-system interaction process. The procedures are represented within the model thanks to the CTA (Cognitive Task Analysis) [3] which splits every step in simple tasks. For each of them it identifies the fundamental cognitive functions. In our reliability representation model every procedure is converted into the fulfillment of a precise number of key cognitive functions. The influence of other external elements like, for instance, environment work shifts, will be considered later on.

Summarizing, the model proposed doesn't represent operators reliability itself, but reproduces the interaction process between man and system.

3. THE CASE STUDY

The study was performed analyzing a chemical production plant, owned by a worldwide enterprise. In particular has been considered a part of the phtalic-anhydride production cycle [4], putting the attention on the refrigeration system of the reactor.

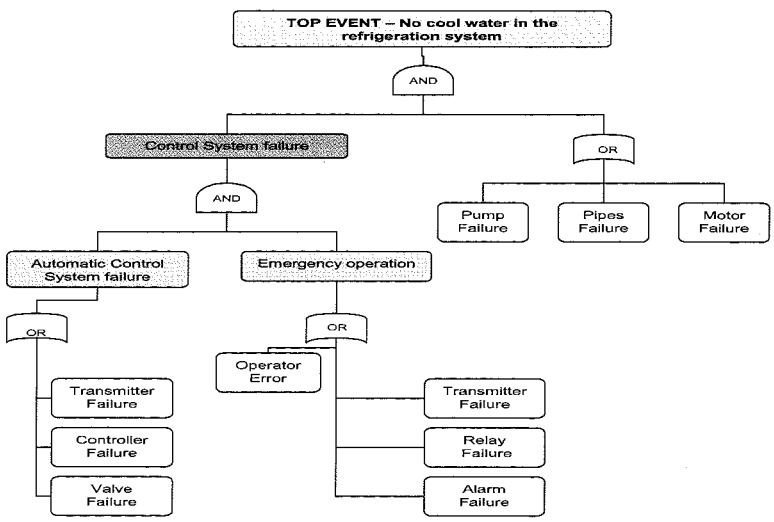
Figura 1 : Phatlic – anhydride production cycle



The reactor, as shown in figure 1, is cooled by a salts circuit that is chilled, in its turn, by a water circuit, connected by an heat exchanger. The present application regards the water circuit. It is composed by three process components: the electrical motor, the pump, the piping with the heat exchanger. These elements are monitored by a control system whose aim is to avoid that a breakdown in the salts refrigerating system could cause a dangerous reactor temperature growth. The main process variable is the temperature, its control and management is essential to obtain a chemical product with the required properties and to avoid dangerous events. The presence of the operator, in parallel with the automatic control system, is requested considering the severity of the possible accidents.

Cooling process is monitored in a control panel room where diagnostic signal arrives. Each machine failure or system breakdown causes an automatic process stop by means of turning off the reactor. If this automatic system fails for whatever reason, there is a standing by manual system which will stop the reaction. Manual stopping action is composed by two steps: first step is in the control room where the operator should check the system failure and the second step is on the plant where another operator, activated by a phone call of the first one, should close the inlet reactor valve. Since operators belong to eight hours work shifts rotating during the 24 hours, we had to consider the presence of three different teams. Each team is composed by a control panel operator and a worker in field.The control system of the circuit has a sensor that control the fluid flow in the pipes. In the standard operative condition such an instrument checks the flow in the cool water circuit and acts on a regulation valve. Moreover, if for any reason there isn't flow in the pipes, it is able to stop the reaction process operating on the reactor inlet valve. We considered as an alarm a warning event that is not managed by the automatic control system and thus requires an action performed by a human being. It happens when automatic control system fails and operators are called to operate. The preliminary control system study was performed using an FTA [5] shown in figure 2.

Figure 2 : Fault tree analysis related to control system



The corresponding control system RBD [5], shown below, was built using the reliability data obtained from FTA.

Figure 3 : Control system RBD

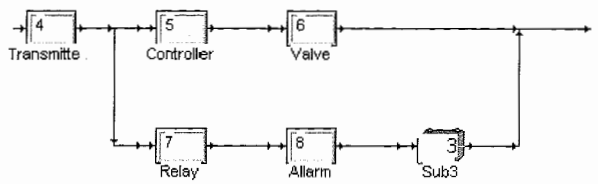
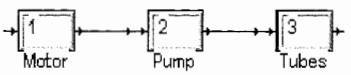


Figure 4 : Mechanical components RBD



In Figure 3 is shown the control system RBD. The item called Sub3 represents the human interaction model, better explained in Figure 6.

4. THE ASSESMENT METHODOLOGY

Simulation is the methodology used to approach the study and the simulator software chosen is SPAR [6] (produced by ClockWork Group). SPAR is a maintenance process simulator characterized by a great flexibility and is able to:

- Represent a very large number of work timetables;
- Manage numeric values uncertainty;
- Modify system logics during the simulation runs.

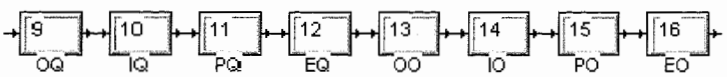
Moreover it is also possible to create some code lines to build up logic and model not available in the standard program tools.

The system implementation in the process simulator required the following steps:

- Reliability Block Diagram (RBD) construction;
- Mechanical and electrical blocks definition by reliability values and data (MTBF, MTTR, maintenance policies man maintenance inspections);
- Creation of management logics by some code lines with the Bubble Maker tool.

Human factor influence is introduced by procedures that represent the sequence of operations that human operators have to do. In every task it is possible to recognize cognitive activities and basic cognitive functions. Using SPAR we created an RBD in which we had to model cognitive functions as a serial or parallel set of block. Considering that human operators should complete all the cognitive functions requested from their tasks, the overall cognitive functions would be represented by a serial system.

Figure 5 : Procedure and cognitive functions RBD



It was necessary to attribute to each block a failure rate. In the case of cognitive functions we used a failure rate obtained using historical data from scientific literature and a numerical index derived from the application of a cognitive model.

$$\lambda_{Tcf\,z} = n \cdot i_v \cdot \sum_{j=1}^{l} \lambda_{j\,z} \qquad (1)$$

Where λ_{Tcf} is the theoretical cognitive function failure rate and it comes from the product of the following terms:

- n is the cognitive function occurrence in a single procedure (Figure 6);
- i_v is the average procedure evaluation index for each cognitive function (Figure 6);

- $\lambda_{j\,z}$ are the nominal values of cognitive function failure modes [7] for each one of the z (four) cognitive functions.

The numerical index (i_v) is obtained analyzing the procedure used by the operator through HTA-Hierarchical Task Analysis [8]. For each task identified it is possible to recognize the cognitive activities and the cognitive functions. Evaluation index is assigned to each cognitive function using a methodology derived from the CREAM (Cognitive Reliability and Error Analysis Method) [7] in order to obtain a cognitive demand profile which represents the cognitive load that each operator should assure.

Figure 6 : Cognitive functions evaluation indexes and occurrence

PANEL CONTROL OPERATOR

STEP N°	TASK	Cognitive action	cognitive function O p	O r	O i	I c	I v	I d	P d	P e	P c	E v	E s	E f	evaluation indexes f_O	f_I	f_P	f_E
1	System monitoring	monitoring	3	3	3	3	3	3							1,00	1,00		
2,1	Alarm type definition	identification				0	3	3								0,67		
2,2		diagnosis				3	0	3	3	3	3					0,67	1,00	
3,1		evaluation				3	0	3	3	0	3					0,67	0,67	
3,2	Action plan definition	planning							3	3	3						1,00	
4,1	Calling operator in field	identification				3	0	3								0,67		
4,2		communication				3	0	3				3	0	0		0,67		0,50
4,3		verification	0	3	3	0	3	0							0,67	0,33		
5																		
6,1																		
6,2																		
6,3																		
COGNITIVE DEMAND PROFILE															0,83	0,67	0,89	0,50
COGNITIVE FUNCTIONS OCCURRENCE			2	2	2	7	7	7	3	3	3	1	1	1				
			15,4%			53,8%			23,1%			7,7%						

OPERATOR IN FILED

STEP N°	TASK	Cognitive action	cognitive function O p	O r	O i	I c	I v	I d	P d	P e	P c	E v	E s	E f	evaluation indexes f_O	f_I	f_P	f_E
1																		
2,1																		
2,2																		
3,1																		
3,2																		
4,1																		
4,2																		
4,3																		
5	Receive action to act	identification				3	0	3								0,67		
6,1	Actions	observation	0	3	3										0,67			
6,2	communicated	identification				3	3	3								1,00		
6,3	execution	execution										0	0	6				1,00
COGNITIVE DEMAND PROFILE															0,67	1,00	0,00	1,00
COGNITIVE FUNCTIONS OCCURRENCE			1	1	1	2	2	2	0	0	0	1	1	1				
			25,0%			50,0%			0,0%			25,0%						

Human reliability depends on the operator really present in the system in every work shift, so we had to consider also the real cognitive profile available and eventually possible gaps in comparison with the cognitive demand profile [9].

Figure 7 : Demand and available cognitive profiles related to panel control operator

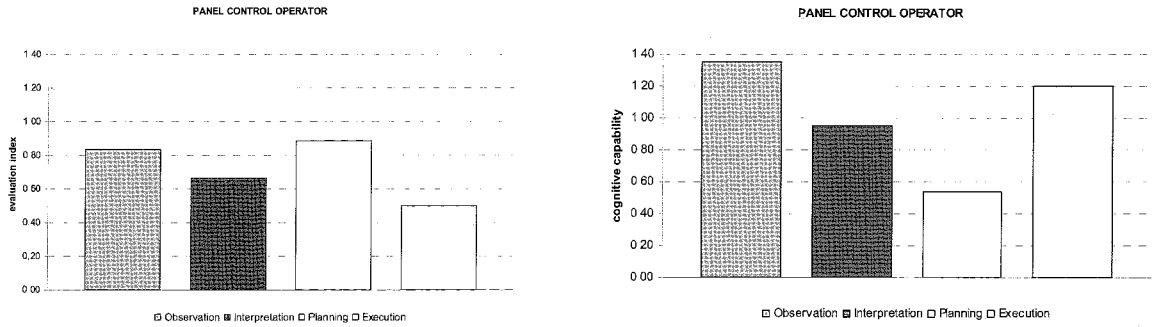
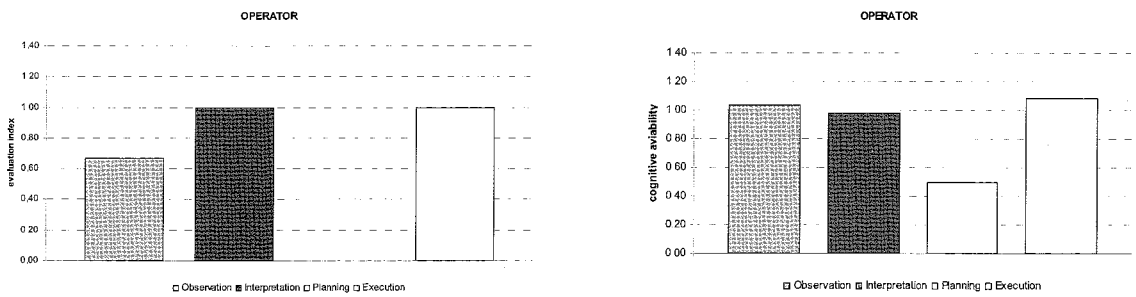


Figure 8 : Demand and available cognitive profiles related to operator in field



If cognitive available profile is lower than cognitive demand, the corresponding cognitive function failure rates are increased with the same proportion, called α.

$$\alpha_z = \frac{Freq_z - Faval_z}{Freq_z} \quad \text{with z = 1 to 4 (cognitive functions)} \tag{2}$$

$$\lambda_{Rcf\,z} = \lambda_{Tcf\,z}(1+\alpha_z) \tag{3}$$

$\lambda_{Rcf\,z}$ is the real cognitive function failure rate

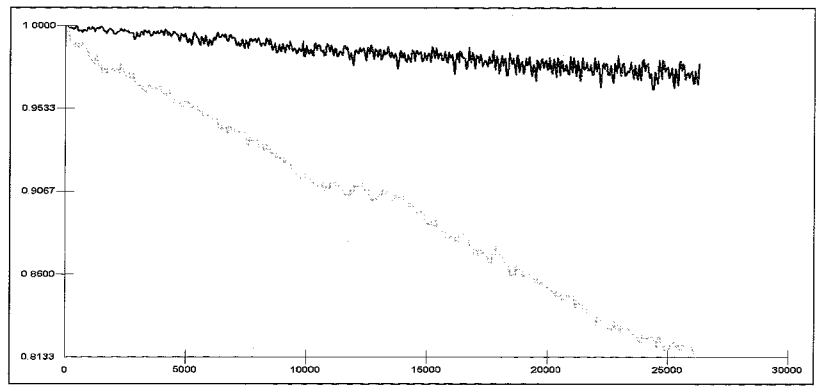
5. THE SIMULATION RESULTS

Results come from 1500 simulation runs and each history lasts 28680 hours, that is equal to an operating mission profile of three years for a continuative 24 hours cycle. It was made a comparison between the two different configurations of the monitoring system:

1. only automatic control (ACS – Automatic Control System);
2. parallel by automatic control and operators check (AMCS – Automatic and Manual Control System).

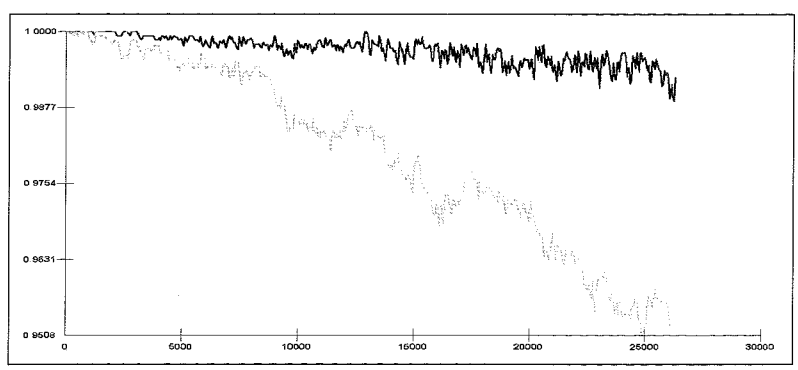
In the following graphs the performance indexes, reported always on y axis, are respectively indicated by a dark blue line for first configuration and a light green line for the second one. On the x axis there is the operating time. In picture 9 the ACS and AMCS probabilities of correct working are plotted. As shown, the control system with the human element is significantly safer.

Figure 9 : ACS and AMCS probabilities of correct working



The operating average probability increases from 0,89 to 0,98 with a last value of about 97% of the AMCS versus 81% of the ACS. The control system, therefore, has increased its reliability performance of about the 10% thanks to the introduction of the human controllers. The lower gradient of the AMCS reliability is bound to the human element whose performances are renewed in every work shift while the mechanical and electromechanical components are subjected to ware out processes. Anyway the ACMS probability still decreases because the human elements is only one item inside a more complex system. The cognitive model shows that in the 10% of the cases of required intervention there may be a operators' mistake within the cognitive functions. Considering not only the control systems but the whole cooling system, the simulation results are shown in picture 10 where the probability of an uncontrolled failure event are presented. The light line is the ACS one and the dark is the AMCS. As visible, the human element yields a significant increase of the overall probability of being in an under-control status, wich goes from 97% to 99%.

Figure 10 : The overall system probabilities of correct working



The simulation showed that during the three years of operation, the system fails about four times and that 98% of this events the control system is able to detect the breakdown and will stop the reaction. Without the human element the last percentage is of about 89%. This means that every 8 years relevant accident would happen instead of one every 40 years with the operator.

6. THE CONCLUSIONS

The simulation results show qualitatively how important was the human control in the case study, reducing the dangerous situations. Moreover a numerical evaluation of the increased probability of having the system under-control, gave a quantitative first approximation of how better the second situation is. Our proposal wasn't to give a numerical estimate of the human reliability itself but to appreciate only the human behaviour within a few well defined operating procedures.

This effort was made because we had a reliability evaluation of a electromechanical control system and we needed to foresee the usefulness of the introduction of the human beings. The present might be a possible way to be follow whenever it was necessary to conduct a feasibility study related to the introduction of human operators with control tasks.

References

[1] James Reason, "*Human Error*", Cambridge University Press, 1990.

[2] Barry Kirwan, "A Guide to Pratical Human Reliability Assessment", London Taylor & Francis, ltd., 1994.

[3] Wayne W. Zachary, Joan M. Ryder, James H. Hicinbothom "*Cognitive Task Analysis and Modeling of Decision Making in Complex Enviroments*", J. Cannon-Bowers & E. Salas (eds.).

[4] Irene Cappelli, "*La manutenzione negli impianti di processo a rischio di incidente rilevante: aspetti tecnici e organizzativi*", Tesi di Dottorato, Università degli Studi di Firenze, Dipartimento di Energetica, Sezione Impianti e Tecnologie Industriali, 2004.

[5] Center for Chemical Process Safety, "*Guidelines for Hazard Evaluation Procedures*", American Institute of chemical Engineers, 1992.

[6] ClockWork Group "*SPAR 5.1 Handbook*", 2003.

[7] Erik Hollnagell, "*Cognitive Reliability and Error Analysis Method – CREAM*", Elsevier, 1998.

[8] Kirwan, B. & Ainesworth, L. K. (eds.), "*A Guide to Task Analysis*", London Taylor & Francis, ltd., 1992.

[9] Mario Tucci, Lorenzo Giagnoni, Marcello Mossa Verre, Francesca Tocchi, "*Criteri per la valutazione dell'affidabilità umana negli impianti di processo*", Convegno nazionale valutazione e gestione del rischio negli insediamenti civili ed industriali, VGR 2004, 19-21 Ottobre 2004, Pisa.